ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. All records pertaining to violations of the following statutes: knowing possession of child pornography, 18 U.S.C. § 2252(a)(4)(b), knowing transportation of child pornography, 18 U.S.C. § 2252(a)(1), and knowing receipt and distribution of child pornography, 18 U.S.C. § 2252(a)(2), including:

a. Records and information constituting or relating to images or videos of suspected child pornography;

b. Records and information relating to communications between individuals about child pornography, to include any communications soliciting child pornography;

c. Records and information relating to the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography;

d. Records and information relating to membership in online groups, clubs, or services that provide or make accessible child pornography to members;

e. Records and information relating to any e-mail accounts used to view, access, trade or distribute child pornography;

f. Records and information relating to communications with Internet Protocol address 209.99.193.74;

g. Records and information relating to malicious software, or which reflect the absence of malicious software;

h. evidence of who used, owned, or controlled the Target Media at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

i. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

j. evidence of the attachment to the Target Media of other storage devices or similar containers for electronic evidence;

k. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Target Media;

l. evidence of the times the Target Media was used;

m. passwords, encryption keys, and other access devices/media that may be necessary to access the Target Media;

n. records of or information about Internet Protocol addresses used by the Target Media; and

o. records of or information about the Target Media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.